Statement of

Mr. Lawrence Castro

Managing Director, The Chertoff Group

to the

House Energy and Commerce Subcommittee on Oversight

March 27, 2012

IT Supply Chain Security: Review of Government and Industry Efforts

Good Morning Chairman Sterns, Representative DeGette and members of the Subcommittee.

I appreciate the opportunity to speak with you today regarding the important role of IT supply chain security in our nation's approach to cybersecurity. I would like to state clearly that I am appearing today in my personal capacity, although, for the record, I am currently a Managing Director at the Chertoff Group, a global security and risk management firm that provides strategic advisory services on a wide range of security matters, including cybersecurity and the supply chain security component of cybersecurity.

While my work at The Chertoff Group certainly informs much of my current insight into the cybersecurity threat environment and the challenges faced by our nation's national security and homeland security sectors, my basic understanding of information assurance and cybersecurity is drawn from my 44 years of Federal service at the National Security Agency. It is from these two perspectives that I offer my views for your consideration today.

I would like to commend the subcommittee for addressing the topic of cybersecurity generally in its hearings and the supply chain security issue specifically today. As the GAO report that was reviewed at the outset of this hearing so well describes, securing the supply chain of products destined to be employed in Federal national security and national security related information systems is a complex task with many moving parts and dependencies. I would suggest, however, that it is not an intractable problem and it is one that can be addressed in a classic risk management framework.

SUMMARY OF PAST WORK

As I noted, the GAO report under discussion today provides both an excellent overview and problem statement. Other efforts have also contributed to the body of literature related to this critical area.

- As the subcommittee's background paper notes the 2008 Comprehensive National Cybersecurity Initiative (CNCI) identified supply chain risk management as one of the effort's 12 critical initiatives.
- The Administration earlier this year published the National Strategy for Global Supply Chain Security[1]. While addressing issues broader than IT, the strategy does provide a range of policy goals that are the basis for further action.
- Two Departmental efforts that were completed in the interim are noteworthy:
  - During Panel One you heard from Mr. Komaroff who leads DoD's Trusted Mission Systems Networks effort that was established by DoD Directive-Type Memorandum 09-016 on March 25, 2010[2].
  - Additionally, in June 2010 NIST completed and documented[3] a comprehensive set of supply chain risk-mitigating best practices that could be applied on a pilot basis to 'jumpstart' specific Department or Agency efforts.
- The private sector has been active in this area as well. In addition to the Open Group's work which is being discussed today, the Internet Security Alliance has published draft guidelines for securing the supply chain for electronic components[4].

Thus, there is ample policy direction and implementing guidance from which one can start to build supply chain defenses. What is needed, however, is a framework that can build on the policy base and also can support the implementation detail. Risk management offers such a framework.

APPROACHING SUPPLY CHAIN SECURITY THROUGH A RISK MANAGEMENT CONSTRUCT

Risk management approaches security from the aspects of threats, vulnerabilities and consequences, and can be used to unwrap some key supply chain issues.

[1] The White House, *National Strategy for Global Supply Chain Security*, January 23, 2012

[2] DTM 09-016, Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems, March 25, 2012

[3] NIST draft NISTIR 7622, *Piloting Supply Chain Risk Management Practices for Federal Information Systems*, June 2010

[4] Internet Security Alliance (ISA), *The ISA Guidelines for Securing the Electronics Supply Chain*, Draft Version 6, 2011.

Threat Actors

Let's first consider who might both be able to benefit from and execute an infiltration of the supply chain, perhaps by successfully inserting a modified component into the supply chain of a critical U.S. government IT enterprise. To do so, an adversary must be capable of penetrating the production process at a point far enough downstream in the process to ensure the right target has been infiltrated. In addition to performing the adversary's desired covert function, the modified component must also precisely execute the component's function as originally designed. I submit that across the spectrum of threat actors active in cyberspace, the most likely players to have the motive and the capability to successfully accomplish such a deception would be nation states. The simple substitution of counterfeit components capable of performing the original design intent but which present the risk of lower reliability or performance must not be overlooked, but I believe it is of secondary consideration.

Who then would be the nation states that have the necessary qualifications and motives? The GAO report notes the existence of an outstanding organization which is on point within the Federal Government for identifying such threat actors. This organization is the Office of the National Counterintelligence Executive (NCIX) within the Office of the Director of National Intelligence. In October 2011, NCIX published an eye-opening report to Congress entitled "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace".[5] The report convincingly presents the case that both the People's Republic of China and the Russian state apparatus have both the intent and capability to undertake economic espionage enhanced by cyber means. The Chinese and the Russians, therefore, are the key threat actors against whom our supply chain defenses must be aligned.

Consequences

What then do these nation state adversaries seek to achieve by compromising the U.S. supply chain? The scope of objectives spans the full range of those who engage in malicious activity in cyberspace:

- **Compromise of Confidentiality** leading to the loss of sensitive data and intellectual property (IP).
- **Loss of Availability** resulting from sabotage of Internet-enabled technologies and critical communications systems.
- **Degradation of Data Integrity** that would result in lack of confidence in sensor or weapons systems-related data in the lead up to or during conflict.

[5] Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*: *Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011.* October 2011.

The NCIX report gives prominence to the extensive loss of IP resulting from Chinese and Russian cyber espionage activity, and this most certainly is the near-term consequence of concern. The loss of availability and data integrity, however, are longer-term impacts which must be acknowledged in building the defensive strategy.

Vulnerabilities

There are numerous vulnerabilities in supply chains for both hardware components and supporting software that the sophisticated nation state adversary can pursue. As noted earlier, there are both NIST and industry best practices and tools that may be implemented to address these vulnerabilities. Additionally, the DHS National Cybersecurity Division's (NCSD) Supply Chain Risk Management Program (also described in the GAO report) offers government users an array of useful services to apply. The use of these tools and resources, however, must be considered in the context of the likely threat actors and the consequences they seek to achieve in executing what is certainly an extensive, resource intensive, intelligence-driven covert action by our potential adversaries.

HOW IT ARCHITECTURE CAN ADDRESS THE THREAT

For IT enterprises either in operation or under design, considerations of system architecture can contribute to supply chain risk mitigation. Two such considerations are worthy of discussion.

Presumption of Breach

This concept, first announced last summer in the DoD Strategy for Operating in Cyberspace[6], posits that one should begin considerations of cybersecurity with the assumption that one's network is already breached and as such, must employ defenses capable of "operating under attack". Such a notion is a powerful one that requires the cyber defender to consider defense mechanisms beyond the standard firewall/anti-virus regime and good computer user hygiene.

Data Centric Defense

If one begins with the premise that a supply chain vulnerability has been exploited and as a consequence the adversary is now present in the IT enterprise, one is quickly driven to the following approach to protect against the loss of critical information:

[6] *Department of Defense Strategy for Operating in Cyberspace*. July 2011. http://www.defense.gov/news/d20110714cyber.pdf

- First, it is necessary to catalog and consolidate the information that is determined to be the most critical to the operation of the element the IT enterprise supports. These are the so-called “crown jewels”.
- Next, one establishes virtual enclaves within which this mission critical data is stored and is afforded special protection (e.g. by encrypting data at rest).
- Access to this critical data is then restricted by robust authentication mechanisms to only those with a “need to know”. The activity of these users is strictly monitored, particularly with regard to movement of this critical data outside of the protected enclave.

Thus, even though the adversary may have established a presence within our network and gained the privileges of a legitimate user, attempts to steal and exfiltrate data will be detected.

INTELLIGENCE AND INFORMATION SHARING AS AN ENABLER

Finally, I would like to comment about a section of the GAO report dealing with “lineage” of equipment and software used in U.S. government networks. The report concluded that emphasis is not given to determining if such networks contain foreign-developed equipment or software, or are supported by foreign-based services. The report noted that both ODNI and NSA representatives offered the view that determining if a relationship exists between a supplier company and a foreign military or intelligence service is a more reliable indicator of a potential security risk than whether a product was manufactured or provisioned outside the United States. I would strongly endorse this conclusion and would note that the practice of conducting “due diligence” audits of such links is well established in private sector best practices and is currently based primarily on open source information.

The challenge, of course, is that for maximum effectiveness, this “due diligence” requires a good conduit of threat actor information between the U.S. Intelligence Community, which has the highest fidelity information in this regard, and those in the private sector who would benefit from the Intelligence Community’s insights. It is encouraging that many of the cybersecurity bills under consideration by the Congress address the need for such improved information sharing.

Again, thank you for the opportunity to address this critical topic and I would be pleased to address your questions.

###